HIPAA Omnibus Rule: Compliance Checklist

The new HIPAA omnibus rule modifies the privacy and security rules for covered entities, and their business associates. Although the new rules are effective March 26, 2013, covered entities and business associates generally have until September 23, 2013 to comply. Before then, covered entities and business associates need to do the following:

1. **Business Associates: Implement HIPAA Policies, Procedures and Safeguards.** The HIPAA privacy and security rules now apply directly to business associates of covered entities. "Business associates" are those outside entities that create, receive, maintain or transmit protected health information in the course of performing functions on behalf of a covered entity, including contractors, consultants, data storage companies, health information organizations, and subcontractors of business associates. Business associates must now implement many of the same policies, procedures and safeguards that have been required of covered entities for years, including the following:
    a. **Security Rule.** Business associates will need to conduct and document a risk assessment of their information technology systems and implement the specific administrative, technical and physical safeguards specified in the Security Rule. The Office of Civil Rights' website contains helpful guidance for Security Rule compliance.
    b. **Privacy Rule.** Most of the privacy rule provisions do not apply directly to business associates, but because business associates cannot use or disclose protected health information in a manner contrary to the limits placed on covered entities, business associates will need to implement many of the same policies and safeguards that the Privacy Rule mandates for covered entities, including rules governing uses and disclosure of protected health information and patient rights concerning their information. Those are typically outlined in the business associate's agreement with the covered entity. Since business associates are now directly liable for HIPAA violations, they should ensure they understand and train their employees concerning HIPAA Privacy and Security Rule requirements.
    c. **Breach Notification.** If a business associate becomes aware of a breach of unsecured health information, they must notify the covered entity and assist the covered entity in responding to the breach.
2. **Identify New Business Associates and Execute Agreements.** Covered entities are required to have business associate agreements with their business associates before allowing them to use or disclose protected health information. The omnibus rule expanded the definition of "business associates" to include entities that provide data transmission services and require routine access to information such as health information organizations. Covered entities should identify any such business associates and execute appropriate agreements with them. Business associates must execute appropriate business associate agreements with their own subcontractors if the subcontractor creates, receives, maintains or transmits protected health information for the business associate.
3. **Review and, If Necessary, Amend Business Associate Agreements.** Covered entities and business associates must ensure that their existing and future agreements contain the elements required by 45 CFR § 164.314(a) and .504(e). In addition to previous requirements, the agreement must require the business associate to:
    a. Comply with the security rule.

b. Execute business associate agreements with their subcontractors.
c. To the extent the business associate carries out on obligation of a covered entity, comply with any HIPAA rule applicable to such obligation.
d. Report breaches of unsecured protected health information to the covered entity.

The OCR has published updated sample business associate language here. The omnibus rule confirms that covered entities are liable for the misconduct of business associates if the business associate is acting as the agent of the covered entity. To minimize their exposure, covered entities and business associates should ensure their agreements confirm that their business associates and subcontractors are acting as independent contractors and not as the agents of the covered entity or business associate, and that the agreements do not give the covered entity too much control over day-to-day operations of the business associate. Covered entities have up to September 22, 2014 to modify business associate agreements if (1) the agreement they had in place on January 25, 2013, complied with the HIPAA rules as of that date, and (2) the agreement does not expire or renew prior to September 22, 2014.

4. **Update Privacy Policies.** Covered entities should update their privacy policies to comply with the new omnibus rules, including the following as applicable to the covered entity:
    a. **Deceased Persons.** Covered entities may now disclose protected health information to family members or others who were involved in the decedent's health care or payment for their care prior to the decedent's death so long as the disclosure is relevant to the person's involvement and is not inconsistent with the decedent's prior expressed wishes.
    b. **Patient Access to Electronic Information.** If a patient requests an electronic copy of their information, covered entities must generally produce it in the form requested if readily producible. If the patient directs the covered entity in writing to transmit a copy of the electronic information to another person, the covered entity must generally comply.
    c. **Response to Request for Access.** Covered entities must generally respond to a patient's request to access their information within 30 days.
    d. **Limits on Disclosures to Insurers.** Covered entities cannot disclose information about a patient's care to an insurer if (1) the insurer seeks the information for treatment or payment purposes; (2) the patient or someone on the patient's behalf paid for the care to which the information pertains; and (3) the patient requests that the information be withheld from the insurer. Developing a workable solution may take some advance preparation. Fortunately, the limit only applies if a patient requests nondisclosure; most patients will not request this restriction unless asked, so covered entities should not raise the issue with the patient. If a patient does request nondisclosure, covered entities should require that such requests be directed to a central person who can coordinate the efforts among billing, medical records, IT, and other relevant departments to ensure the protected data is sequestered.
    e. **School Immunizations.** Covered entities may now disclose information about immunizations to a school if (1) state law requires such information for school enrollment; and (2) the patient or their personal representative consents to the disclosure.

   f. **Sale of Information.** Covered entities must obtain written authorization to sell a patient's information, and the authorization must disclose that the sale will result in remuneration to the covered entity.
   g. **Marketing.** Covered entities must obtain written authorization to use the patient's information for marketing purposes, including most non-face-to-face communications for treatment purposes if the covered entity receives financial remuneration to make the communication. If remuneration is involved, the marketing authorization must disclose that fact.
   h. **Fundraising.** The new rule allows covered entities to disclose more information to institutionally related foundations to assist with fundraising, but fundraising communications must explain how the recipient may opt out of receiving such communications and the opt out method cannot be burdensome.
   i. **Research.** If the covered entity engages in research, it should review new standards applicable to research as described in 45 CFR § 164.508(b).
5. **Update Breach Notification Policies.** The omnibus rule modified the standard for reporting breaches of unsecured health information. Under the new standard, the unauthorized acquisition, access use or disclosure of protected health information in violation of the Privacy Rule is presumed to be a reportable breach unless (1) the covered entity or business associate demonstrates there is a low probability that the information has been compromised based on a risk assessment of certain factors, or (2) the breach fits within certain exceptions. Covered entities must ensure that their policies incorporate and that they apply this new, arguably lower standard. Given the lower standard, covered entities and business associates may want to consider encrypting records to the extent possible to avoid reportable breaches.
6. **Modify Notice of Privacy Practices.** Covered entities must update their notices of privacy practices to add the following:
   a. A description of the types of information that require an authorization, i.e., psychotherapy notes, marketing, and sale of information.
   b. A statement that other uses or disclosures not described in the notice will require an authorization.
   c. A statement that the recipient of fundraising materials may opt out.
   d. A description of the individual's right to limit disclosures to insurers if the patient paid for the relevant care.
   e. A statement that the covered entity must notify the patient of a breach of unsecured protected health information.
7. **Train Employees.** Covered entities and business associates must train their employees concerning the new rules.
8. **Review HIPAA Compliance.** Given the new, lower breach notification standard, covered entities will likely to be required to self- report more breaches. Those reports may result in more patient complaints and government investigations. Accordingly, it is a good time to review and, as necessary, improve your compliance with all the HIPAA rules, not just the new omnibus rules. Doing so may help you avoid reportable breaches and, if a breach occurs, sidestep HIPAA penalties, which can range from $100 to more than $50,000 per violation. Having the required policies and safeguards in place coupled with prompt action to correct any breach will likely establish an affirmative defense to any penalties.